SUPERIOR COURT OF <Enter your state here>

County of <Enter your county here>

SEARCH WARRANT

<Enter your full name here> swears under oath that the facts expressed by him in the attached and incorporated **Statement of Probable Cause** are true and that based thereon he has probable cause to believe and does believe that the articles, property, electronic communications, and data described below are lawfully seized pursuant to <code> et seq., as indicated below, and are now located at the location(s) set forth below. Wherefore, Affiant requests that this Search Warrant be issued.

_____

(Signature of Affiant)

THE PEOPLE OF THE STATE OF <Enter your state here> **TO ANY PEACE OFFICER IN THE COUNTY OF** <Enter your county here>: proof by affidavit, having been this day made
before me by <Enter your full name here>, finds that there is probable cause to believe that the property and/or person described herein may be found at the locations set forth herein and is lawfully seized pursuant to <code> et seq., as indicated below by **X** (s) in that:

- When the property was stolen or embezzled;
- When the property or things were used as the means of committing a felony:
- When the property or things to be seized consist of an item or constitute evidence that tends to show that a felony has been committed, or tends to show that a particular person has committed a felony;
- When the property or things are in the possession of any person with the intent to use them as a means for committing a public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery;
- There is a warrant to arrest a person;
- When a provider of electronic communication service or remote computing service has records or evidence, as specified in <code>, showing that property was stolen or embezzled constituting a misdemeanor, or that property or things are in the possession of any person with the intent to use them as a means of committing a misdemeanor public offense, or in the possession of another to whom he or she may have delivered them for the purpose of concealing them or preventing their discovery;

PLACE TO BE SEARCHED:

See Attachment A

ITEMS TO BE SEIZED:

See Attachment B

Attachment "A"

YOU ARE THEREFORE COMMANDED TO SEARCH:

Google, LLC – An Electronic Communications Service Provider
Google Legal Investigations Support
1600 Amphitheatre Parkway
Mountain View, CA, 94043

Service via Google's Law Enforcement Request System (LERS) on-line
Service may be via email at uslawenforcement@google.com

Attachment "B"

ITEMS TO BE SEIZED AND SEARCHED:

This warrant is directed to Google, LLC, headquartered at 1600 Amphitheatre Parkway, Mountain View, California, and applies to:

Records pertaining to:

Identifying information according to the "**Production Protocol**" described below for Google accounts that reported a GPS, cellular, WiFi or Bluetooth sourced location history data generated from devices that reported a location within the geographic region bounded by the following coordinates dates and times ("**Initial Search Parameters**"):

Search 1:

Date and Time Period:
<Enter start date and time> to <Enter end date and time>

Target Location:
A radius of <enter radius> meters around Latitude <enter latitude>, Longitude <enter longitude>.The area is further described as the immediate area around <address, city and state> and is pictured in the following image:

Image 1:

Production Protocol:

1. Google shall query location history data based on the **Initial Search Parameters** (as described above).
2. For each location point recorded within the **Initial Search Parameters**, Google shall produce anonymized information specifying the corresponding unique device IDs of all location data, whether derived from Global Positioning System (GPS) data, cell site/cell tower triangulation/trilateration, Bluetooth beacons, precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates, estimated radius, and the dates and times of all location recordings (with captured time zone), data source and device type (platform), during the date and time period associated with specific device IDs; (the "**Anonymized List**").
3. Law enforcement shall review the **Anonymized List** to remove device IDs that are not relevant to the investigation, for example, device IDs that were not in the location for a relevant period of time, or device's that remained at the location after law enforcement arrival. Law enforcement will also shortlist the Anonymized List by reviewing the time stamped location coordinates for each device ID and compare that against the known time and location information that is specific to this crime. Law enforcement will also compare the Anonymized List for each location and attempt to locate device IDs located at two or more identified locations.
4. If additional location information for a given anonymized device ID is needed in order to determine whether that anonymized device ID is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the time period that fall outside of the **Initial Search Parameters**. These contextual location coordinates may assist law enforcement in identifying anonymized device IDs that were located outside the search locations, were not within the search locations for a long enough period of time, were moving through the search locations in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

<Special note: It is our recommendation to use a second legal demand when seeking subscriber data. If you proceed with subscriber data under one legal demand, you can leave PP #5. Be sure to remove PP #5 if using a second warrant as well as any language in the body of the warrant related to subscriber data. See instructions tab for details; special attention California agencies. Be sure to check with your prosecutors before moving forward>

5. For those anonymized device IDs identified as relevant pursuant to the ongoing investigation through an analysis of provided records, and upon demand by law enforcement, Google shall provide identifying information for the Google accounts associated with each identified anonymized device IDs, to include subscriber's name, street address, telephone number(s), email addresses, services subscribed to, last six (6) months of IP history, SMS account number, and registration IP, all information provided by the subscriber to the service provider to establish or maintain an account or communications channel.

Investigating officers and those agents acting under the direction of the investigating officers are authorized to access all data to determine if the data contains the items as described above. Those items that are within the scope of this warrant may be copied and retained by investigating officers.

Order for Production of Records

It is hereby ordered that any records produced in response to this search warrant may be provided via email or digital storage media to:

<Enter your full name here>
<Enter your address here>
<Enter your city here> ,
<Enter your state here>
<Enter your zip here>
<Enter your here>
<Enter your here>

Order to Delay Notice:

<Be sure to include a Non-Disclosure/Delay of Notice since Google's policy is to notify their users of law enforcement requests unless otherwise ordered to not disclose>
This matter having come before this Court pursuant to an affidavit and petition which requests the issuance of an order commanding Google, LLC to not disclose to or notify any person of the existence of the warrant ("criminal process") attached hereto, the Court finds that:

1. The criminal process is issued pursuant to 18 U.S.C. § 2703(b)(1) (search warrant for the content) or 18 U.S.C. § 2703(c)(2) (criminal process for non-content records), therefore the <Enter your agency here> is not requested to provide notice to the subscriber or customer;
2. The Petition is valid pursuant to 18 U.S.C. § 2703 (b); and
3. Per 18 U.S.C. § 2705(a), there is reason to believe that the notification to any person, other than as is necessary to provide the demanded records, documents, data, and/or content of the existence of the criminal process will result in:
    - Endangering the life or physical safety of an individual;
    - Flight from prosecution;
    - Destruction of or tampering with evidence;
    - Intimidation of potential witnesses; or
    - Otherwise seriously jeopardizing an investigation or unduly delaying a trial.

I further state that the other means of preventing the identified results of the aforementioned disclosure or notification are not readily employable because:

- I do not know the true identity of the suspect in this investigation;
- I do not know the current location of the suspect in this investigation;
- I do not know the location of or description of specific evidence the suspect may possess or to which the suspect may have access to;
- I believe the suspect is in the presence of or has access to a victim or vulnerable person (e.g., a child) who may be a victim of the aforementioned crimes being investigated; and/or,
- Other: <enter other>

It is hereby ordered that Google and the executing agency shall delay notification of the existence of this warrant, or the existence of the investigation, to the subscribers or to any other person:

- permanently; or,
- for a period of time not less than <##> days.

STATEMENT OF PROBABLE CAUSE

Summary:

<Briefly explain the purpose of the warrant. Example:
I am currently investigating a <crime> that occurred on <date>. There are no suspects and I have not yet located any witnesses. The purpose of this search warrant application is to authorize the examination of Google location history records from the time and place of the <crime> to identify potential suspects and witnesses.

Affiant's Experience:

I, <Enter your full name here>, being a duly sworn peace officer for the State of <Enter your state here>, have been employed by the <Enter your agency here> for <Enter years of employment> years.

<Insert affiant's law enforcement experience here>

Investigation:

This affidavit is made in support of a search warrant requesting the listed geo-location information as described in Attachment B, related to a criminal investigation of <code(s)> which began on <date> as described below.

<Insert case-specific reasons for choosing those times listed. Example: "Witness Jones reported hearing a single gunshot at 3:40 a.m. Officer Smith discovered the victim's body at 3:45 a.m. and saw no other people in the immediate area. Therefore, I am requesting records from approximately 10 minutes before the murder through the arrival of Officer Smith.">

Google Location History Data:

Based on my training and experience, I know most people in today's society possess cellular phones and other connected devices (e.g. tablets, watches, laptops) used to communicate electronically. I know these devices are capable of sending and receiving communications in many different forms. I know most people carry cellular phones on their person and will carry them whenever they leave their place of residence. I know that cellular phones may include global positioning systems (GPS) and other technology for determining a more precise location of the device.

I know a subject's physical cellular phone often times does not retain all the data relevant to a specific crime. Portions of this data may only be on the Electronic Communications Service Provider's server located in the subscriber's account. Google services are often interconnected with a log-in to a Google account allowing access to many of the other Google services.

Google is also a company which provides electronic communication services to subscribers, including email services. Google allows subscribers to obtain email accounts at the domain name gmail.com and/or google.com. Subscribers obtain an account by registering with Google. A subscriber using the provider's services can access his or her email account from any computer or smart phone/device connected to the Internet.

Google has developed an operating system for mobile devices, including cellular phones, watches and tablets known as Android, that has a proprietary operating system. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first activate a new Android device.

I know nearly every Android powered device has an associated Google account. I also know that Apple iPhone's supports several Google applications, such as Google Search, Gmail, Google Maps, and Google Drive, all of which require a Google account. I also know Google continuously tracks devices with an associated Google account.

Based on my training, experience and conversations I've had with other law enforcement officers and/or from reviewing documentation, I know that Google collects and retains location data on their servers (also known as the "Sensorvault" database) from Android enabled mobile devices, as well as devices supporting Google applications such as Google Search, Gmail, Google Maps, and Google Drive, so long as the location services of the phone are enabled. The location data gathered is stored forever, unless it is deleted by the user. The company uses this information for location-based advertising and location-based search results. Per Google, this information is derived from Global Position System (GPS) data, cell site/cell tower information, Bluetooth beacons, and Wi-Fi access points. While the specific parameters of when this data is collected are not entirely clear, it appears that Google collects this data not only whenever one of their services is activated and/or whenever there is an event on the mobile device such as a phone call, text messages, internet access, or email access, but also when the user is not interacting with the device (e.g. applications running in the background).

Additionally, location information digitally integrated into images, videos, or other computer files sent via the cellular phone can further indicate the geographic location of the account's user at a particular time. Digital cameras, including cameras built into a cellular phone, frequently store GPS coordinates in the metadata of image files, indicating where a photo was taken. These image files may be stored in the account user's Google cloud storage.

Based on my training and experience, I know when a user activates a Google Account, Google will request an associated phone number for the user, to assist in password recovery if a password is forgotten or for security purposes.

Given that almost all cellular phones and connected devices are either supported by Google or support Google software and most people in today's society carry a cellular phone or other connected device on their person at nearly all times, I believe it is likely the suspect(s) involved in this criminal investigation were in possession of at least one cellular phone/device, which was either powered by Android OS or had a cellular phone with a Google application.

Based on my training and experience, suspects involved in criminal activity will typically use cellular phones to communicate when multiple suspects are involved. I am also aware Android based cellular phones report detailed location information to Google, where the geo-location and electronic data is then stored on their servers.

The timeframe of the Google request of <Date and Timeframe (e.g. 12/12/2018, 10pm PDT to 12/13/2018, 7:00am PDT)> will allow investigators to see which Google device IDs were present in the geographic area prior to, during, and after the crime. The information provided by the extended timeframe and times when entering and exiting the geographical area will allow investigators to determine which device IDs require further investigation and which ones do not.

The initial device IDs provided by Google do not include any subscriber information and is provided in an anonymized list.

I believe the information provided by Google will assist investigators in understanding a bigger geographic picture and timeline, which may tend to identify potential witnesses, as well as possibly inculpate or exculpate the account owners. I therefore believe that it is likely that a review of Google's location history will help law enforcement in developing suspect(s) in a felony crime, the crime of <code(s)> and provide possible witnesses to the crime.

As such, I am requesting a list of any Google anonymized device IDs in a geographic area around the <address of target location(s)> in particular, the geographical region(s) identified in Attachment B and the date(s) and time(s) specified. This Application seeks authority to collect certain location information related to Google device IDs that were located within the Target Location(s) during the Date and Time Period (Anonymized List).

The information sought from Google regarding the Anonymized List will potentially identify which cellular phones/devices were near the location where the crime occurred and may assist law enforcement in determining which persons were present or involved in the crime under investigation.

Law enforcement shall review the Anonymized List to remove device IDs that are not relevant to the investigation, such as device IDs that were not in the location for a sufficient period of time. If additional location information for a given device ID is needed in order to determine whether that device is relevant to the investigation, law enforcement may request that Google provide additional location coordinates for the time period that fall outside of the target location. These contextual location coordinates may assist law enforcement in identifying devices that were located outside the target location, were not within the target location for a long enough period of time, were moving through the target location in a manner inconsistent with the facts of the underlying case, or otherwise are not relevant to the investigation.

Google Legal Process Service Location:

On <date>, I confirmed the location where Google accepts service of search warrants by reviewing the www.search.org "ISP List." Based on my experience and discussion with other members of law enforcement, I know that SEARCH is a national non-profit organization dedicated to sharing information and training law enforcement. The "ISP List" is constantly updated and is commonly relied upon by law enforcement to determine the location to send search warrants to a wide range of communications service providers, financial institutions and other record holders.

According to the SEARCH ISP List, Google, LLC accepts search warrants at the following location:

Google Legal Investigations Support
Google LLC
1600 Amphitheatre Parkway
Mountain View, CA 94043
Service may be via email at uslawenforcement@google.com

Productions of Records

Based on my training and experience, I know that the requested records are maintained in electronic format. I also know that Google prefers to produce records in an electronic format and that electronic records are easier for investigators, prosecution and defense to use. Therefore, I request an order that any records be provided in electronic format to the following address:

<Enter your full name here>
<Enter your address here>
<Enter your city here> ,
<Enter your state here>
<Enter your zip here>
<Enter your here>
<Enter your here>

Conclusion:

The facts set forth in this affidavit are based upon my own personal observations, my training and experience, and information obtained during this investigation. Therefore, based on the above facts, I have probable cause to believe, and do believe, that evidence of the commissions of felonies, in violation(s) of <code(s)>, and property related to the commission of said felonies, will be located on the premises described above. I request that a search warrant be issued with respect to the above location for the seizure of said property.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge and belief.

_____ _____
(Signature of Affiant / Date)